The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE ISSUED:

10/08/2014

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Google Chrome that could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There is no known proof-of-concept code available at this time.

SYSTEM AFFECTED:

- Google Chrome Prior to 38.0.2125.101

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium government entities: **High**
- Small government entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple Vulnerabilities have been discovered in Google Chrome, and have been patched in the latest Stable Channel Update. This update addressed multiple bug fixes, security updates, and feature enhancements including the following:

- A combination of V8 and IPC bugs in Google Chrome could allow for remote code execution outside of the sandbox. [CVE-2014-3188]
- Code execution vulnerabilities associated with BASH environment variables (Shellshock vulnerability). [CVEs 2014-6271, 7169, 7186, and 7187]
- Out-of-bounds read in PDFium. [CVE-2014-3189]
- Use-after-free in Events. [CVE-2014-3190]
- Use-after-free in Rendering. [CVE-2014-3191]
- Use-after-free in DOM. [CVE-2014-3192]
- Type confusion in Session Management. [CVE-2014-3193]
- Use-after-free in Web Workers. [CVE-2014-3194]
- Information Leak in V8. [CVE-2014-3195]
- Permissions Bypass in Windows Sandbox. [CVE-2014-3196]
- Information Leak in XSS Auditor. [CVE-2014-3197]
- Out-of-bounds read in PDFium. [CVE-2014-3198]
- Release Assert in V8 bindings. [CVE-2014-3199]
- Various fixes from internal audits, fuzzing and other initiatives. [CVE-2014-3200]

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Security Focus:

http://www.securityfocus.com/bid/70262

http://www.securityfocus.com/bid/70273

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3188

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3189

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3190 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3191

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3192

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3193

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3194

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3195

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3196

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3197

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3198

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3199

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3200

Google:

http://googlechromereleases.blogspot.in/2014/10/stable-channel-update-for-chrome-os.html

http://googlechromereleases.blogspot.in/2014/10/stable-channel-update.html